REMARKS

Applicant respectfully traverses the rejection of claims 1, 4-11, 13-18 and 21-24 under

35 U.S.C. §103(a) as being unpatentable (obvious) over Want '070 in view of Engelmann '906.

The traverse of claim 24 is based on the fact that the Examiner did not present the

required rationale for showing of *prima facie* obviousness of the subject matter of claim 24

(24/23), which subject matter adds to claim 23 the additional limitation,

> wherein the storage means for the access words to the
> applications are included in the memory of the electronic circuit of
> the portable object or in the determined server.

Applicant will now present an explanation of why the remaining claims 1, 4-11, 13-18,

and 21-**23** would not have been obvious from the applied prior art at the time the claimed

invention was made.

First, even though Applicant disagrees with this rejection, Applicant has amended the

independent claims 1 and 23 to define the "determined server" as a "determined <u>remote</u> server".

Next, the object of the claimed invention is to protect the access to personal computer

applications of a computer station connected to an inter-computer communication network, for

example a personalized e-mail or a financial account or other personalized applications.

Normally, this access to personal applications is automatic when a personal portable object is

near to a read unit connected to the station. This object can be preferably a wristwatch, or a

bracelet, necklace, ring, card or badge.

To this end, in the method of claim 1, the identification code specific to the portable object, i.e., the "readable verification word of the memory of the electronic circuit" of the object, has to be searched after transmission to a determined remote server in a checking file of said server. Said "server" is, for example, the watch manufacturer's server which is, in particular, distant/remote from the computer station with the read unit connected to said computer station. If the readable word has been found in the checking file, a password is sent from the checking file to storage means in which "access words...are kept secret by a read and/or write barrier" in order to allow opening the read barrier. Thus, if no password is transmitted from the dedicated server to the storage means, access words are kept secret, thereby guaranteeing the security of personal information stored in the portable object.

There are two checking operations to allow for opening the read and/or write barrier of the storage means. First, the readable verification word of the portable object is checked in a file of the server remote from the computer station before sending a password. Second, the password is checked to the storage means for opening the read and/or write barrier of the storage means. This method allows, in the event of loss or theft of the portable object, said object to be made inactive by ending its validity via any communication means related to the determined server; thus, personal computer applications cannot be opened by the lost or stolen object in inactive state.

Want '070 describes a method and a system for maintaining processing continuity to mobile computers in a wireless network, wherein there is used portable Tabs, such as PDA (active badges), which includes signal transmission and reception means for communicating

wirelessly with read units (radio or IR) connected to computer stations in different rooms. This system is a ubiquitous computing environment, and these computers with tabs work interactively with each other (col. 2, lines 16-20).

The personal tab includes a display for indicating the location of the tab with its wearer in the environment. As the tab-wearer can change location, the tab is provided an additional layer of network addresses for keeping track of the real address of the mobile unit (tab) and forwarding packet addresses to the unit appropriately (col. 3, lines 30-35). With several mobile units, it is necessary also to provide an authorization access to a specific mobile unit for the security (col. 4, lines 24-29).

The essential feature in Want's disclosure/teaching is an "agent" (application interface), which operates primarily for the benefit of its assigned computer (col. 4, lines 64, 65) in order to allow communications between mobile computer (tab) and its applications. The specific application for the mobile unit must be authorized by the agent (col. 5, lines 5-7), partially like feature d) of Applicant's claim 1. The agent maintains a list of authorised users or applications (col. 5, lines 16, 17). For each tab, there is a dedicated process (agent) to handle a variety of tasks exclusively for the specific tab (col. 8, lines 31-34).

Want's tab 26 is used also as a display terminal allowing computer applications to be accessed by the tab while the application resides and executes on a remote host. The tab 26 can also report events, generated by its user, by the pressing of buttons of the tab (col. 7, lines 10-14). This operation is totally different from an opening of a barrier of storage means by a password, as required by feature c) of Applicant's claim 1. Want's tab can communicate

addresses of applications with an identification number in order to allow an agent of a computer station to recognize the personal tab. Thus, the agent is able to control the authorization of any application to request communication with the specific mobile unit which is the personal tab. If some applications are personalised for a specific tab, the <u>agent manages this communication between the tab and the computer application, which is **entirely different** from Applicant's claimed invention.</u>

Contrary to the Examiner's comments relative to claim 1, there is nothing described or even suggested in Want concerning a tab with a storage means which includes <u>a read and/or write barrier</u> to prevent to access to specific applications of the computer without authorization as required by feature c) of claim 1. This barrier can be opened only if a <u>verification word, in a readable part of the storage means, has first been checked in a checking file located in a remote server,</u> connected by the Internet, for example, to the computer station. This method for sending the verification word is <u>automatic</u> since the tab or portable object is located near the read unit. Once the verification word has been found in the checking file of the server, <u>a password from the server is then transmitted to the electronic circuit of the portable object in order to open the read and/or write barrier of the storage means.</u> After that, application addresses can be transmitted from the storage means of the portable object to the computer station to open the personalized applications.

In the Examiner's comments on page 4 of the Office Action, Applicant notes that the tab displays "You Are Here" in order to show the location of the user, which is **different** from the step a) or c) of Applicant's claim 1 in which <u>an automatic connection to the server is established</u>

for checking the readable word in a list of authorized words. Furthermore, Want (col. 7, lines 6-9) does not even mention step b) of Applicant's claim 1. It certainly would **not** have been obvious for a person skilled in the art to deduce step b) from the teaching of said col. 7, lines 6-9.

According to the present invention, there are two password checking operations in order to authorize the opening of personal applications. First, the readable word is checked in the checking file of the remote server, and, second, the password is checked in the storage means to open the read and/or write barrier. This is quite **different** from Want's hardwired network backbone 12.

Want's agent of the computer **cannot** be compared with Applicant's barrier of the storage means of the portable object, because this agent does **not** transmit a password to the tab in order to eventually open a barrier of storage means of said tab. Rather, this agent checks only the number of the tag for allowing a connection to specific applications. Furthermore, Want also does not describe or suggest Applicant's check of the verification word of the portable object in a checking file of a specific server which is not an agent of a computer. This check by a remote server allows, in the event of loss or theft of the portable object, said object to be made inactive by ending its validity via any communication means related to the determined server, and personal computer applications cannot be opened by the lost or stolen object in the inactive state.

Engelmann (newly cited) describes a portable object, such as a wristwatch, which includes several electronic modules to allow wireless communication between the portable object and an external terminal. With this portable object, a person's right of access to an application is checked. Specifically, this portable object is used for systems for controlling

- 13 -

access to industrial sites or public buildings. One electronic module 28 includes, in particular, an antenna to receive and to transmit data, a logic control circuit, and a memory. The module has a high level of operating security with a 32-bit password and a read protected zone for the organization of security. The logic circuit differs from the others by an identification number and a serial number stored in a ROM memory.

However, as a difference from Applicant's claims 1 and 23, Englemann does not even mention a read and/or write barrier, <u>which can be opened by the password transmitted by the remote server after having checked the verification word transmitted by the portable object</u> in the first step.

Thus, the combination of Engelmann and Want is **incapable** of rendering *prima facie* obvious the subject matter of independent claims 1 and 23..

It is to be noted that the features of claim 13, concerning the read unit in a mouse pad, are not even mentioned in Want which describes only the connection of the read unit to the computer station by RS 232.

On page 5, paragraph ii., the Examiner states that "Want is silent about an electronic circuit with a memory", a statement with which the Applicant agrees. In paragraphs iii. and iv. the Examiner attempts to provide a rationale for combining the teachings of Want and Engelmann in an attempt to show *prima facie* obviousness of **only claim 1**.

In the above analysis, Applicant has pointed out the deficiencies in the respective disclosures of Want and Engelmann with respect to the subject matter of claim 1, whereby Applicant respectfully submits that the Want/Engelmann combination is **incapable** of rendering

obvious the subject matter of claim 1, as the combination clearly does not disclose or even suggest all of the limitations of claim 1. Furthermore, it is clear that, even if the teachings of Want and Engelmann were combined, there would **not** be produced the subject matter of claim 1 or subject matter which would have rendered claim 1 *prima facie* obvious to a person of ordinary skill in the relevant art.

As noted by the Examiner, the limitations of claims 21 and 23 track the limitations of claim 1, whereby claims 21 and 23 are patentable at least for the same above reasons explaining why claim 1 is patentable. The remaining dependent claims are patentable for the same reason claim 1 is patentable, and further because of the additional limitations recited in these dependent claims.

Therefore, Applicant respectfully requests the Examiner to reconsider and withdraw the rejection of claim 1 under 35 U.S.C. § 103(a). **N.B.** Even though the Examiner attempted to present the required rationale in support of the rejection of claim 1 based on unpatentability under 35 U.S.C. § 103(a), the Examiner has **not presented** the **required rationale** in support of the statutory rejection of claims 4-11, 13-18 and 21-24, whereby Applicant respectfully submits that the Office Action is **defective** in this regard, as the Examiner presents no rationale for Applicant to rebut. It is clear that the Examiner's bald statements of what Want "teaches" (on pages 5-9 of the Office Action) fail to meet the MPEP's requirement that the Examiner present a **rationale** for combining references and for finding obviousness in the subject matter of any claim rejected under 35 U.S.C. § 103(a). Furthermore, as already mentioned above, the

Examiner does **not present <u>any</u> statement** to support the statutory rejection of claim 24 under 35 U.S.C. § 103(a).

In summary, then, and for the reasons presented above in detail, Applicant respectfully requests the Examiner to reconsider and withdraw the rejection of claims 1, 4-11, 13-18 and 21-24 under 35 U.S.C. § 103(a) as being unpatentable (obvious) over Want '070 in view of Engelmann '096.

However, if for any reason the Examiner feels that the application is not now in condition for allowance with all of claims 1, 4-11, 13-18 and 21-24, Applicant respectfully requests the Examiner to **call the undersigned attorney** to discuss any unresolved issues and to expedite the disposition of the application.
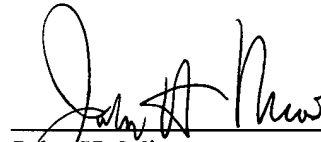
<u>N.B.</u> As noted above, the Office Action is defective in that it does not present any rationale for the rejection of claims 4-11, 13-18 and 21-24 under 35 U.S.C. § 103(a), whereby Applicant respectfully submits that (if the application is not now in condition for allowance) the next Office Action cannot contain a valid "final" rejection of claims 4-11, 13-18 and 21-24.

Filed concurrently herewith is a Petition (with fee) for an Extension of Time of two months. Applicant hereby petitions for any extension of time which may be required to maintain the pendency of this application, and any required fee for such extension is to be charged to Deposit Account No. 19-4880. The Commissioner is also authorized to charge any additional fees

under 37 C.F.R. § 1.16 and/or § 1.17 necessary to keep this application pending in the Patent and

Trademark Office or credit any overpayment to said Deposit Account No. 19-4880.

Respectfully submitted,

John H. Mion
Registration No. 18,879

SUGHRUE MION, PLLC
2100 Pennsylvania Avenue, N.W.
Washington, D.C. 20037-3213
(202) 663-7901

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: October 20, 2005